

REMARKS

Claims 1-24 are all the claims pending in the application. The Examiner finally rejects claims 1-4, 9, 10-14, and 21-23 under 35 U.S.C. §103(a) as being unpatentable over Mroczkowski ("Implementation of the block cipher Rijndael using Altera FPGA," May 2000) in view of Luyster (US 6,182,216). The Examiner further rejects claims 5-8 under 35 U.S.C. §103(a) as being unpatentable over Mroczkowski in view of Luyster and further in view of Daemen et al. ("AES Proposal: Rijndael," March 1999).

§ 103(a) Rejection

Claims 1-4, 9, 10-14, and 21-23 are rejected under 35 U.S.C. §103(a) as being unpatentable over Mroczkowski in view of Luyster, and claims 5-8 are rejected under 35 U.S.C. §103(a) as being unpatentable over Mroczkowski in view of Luyster and further in view of Daemen.

To establish a *prima facie* case of obviousness, three basic criteria must be met one of which is that the prior art reference (or references when combined) must teach or suggest all the claim limitations.¹

Claim 1

Regarding independent Claim 1, independent Claim 1 recites an apparatus for encrypting/decrypting a real-time input stream comprising a control unit, a key schedule unit, and a block round unit wherein the control unit receives a data stream of byte units and converts the data stream into block data. *See*, Application, ¶ [0011]. Applicant amends claim 1 to recite "An apparatus ... comprising a control unit ... a control unit receiving a data stream of byte units wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, converting the data stream into block data" The amendment finds support in paragraph [0030] of the specification.

¹ See, MPEP 2143.

The Examiner states that the control unit receiving a data stream of byte units and converting the data stream into block data was not disclosed in Mroczkowski, and is not explicitly taught in Luyster, but that Luyster inherently teaches converting. Applicants agree that Luyster received a data stream that is already in block form such as 64, 128, or 258 bit blocks as shown in item 50 of Fig. 3. However, Luyster lacks, and does not teach, the structure to convert a stream of byte data into n-bit block data. The Examiner believes this feature is inherent in Luyster. Applicant respectfully disagrees.

However, in order to further the prosecution of the application, Applicant amends the independent claims to recite the additional limitation that the real-time data input stream is a stream of MPEG data or a data feed from a digital satellite service (DSS). Luyster is directed to encrypting or decrypting 128 (or more) bit-blocks of data of plaintext or encrypted plain text. *See*, Luyster, col. 18, lines 54-55. Luyster does not teach decrypting a real time stream of multimedia data, but teaches encrypting or decrypting messages, not a data stream.

Mroczkowski is directed to the underlying mathematics of 128 bit-block ciphers and how they may be implemented in either hardware or software. Mroczkowski does not teach receiving a data stream wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, converting the data stream into block data, and outputting the block data.

According to MPEP § 2143, the third element necessary for establishing a prima facie case of obviousness is that the prior art reference must teach or suggest all the claim limitations. The Examiner has recognized in the Office Action dated January 12, 2006 that Luyster lacks explicit teachings relating the structure to convert a stream of data into n-bit data blocks (“Luyster does not explicitly teach receiving a stream of byte data, it [is] inherent that data is received streamed.”)². Luyster, Fig. 3, item 50, teaches an n-bit block of data for further processing before encryption wherein n is, for example, 64, 128, or 256 bits. Luyster therefore, receives data already formed into blocks of a specific size rather than teaching the limitation of converting the data stream into block data of claim 1. Further, neither Mroczkowski nor Luyster, either taken individually or together, do not teach the limitation that the data stream is an MPEG

² *See*, Office Action dated January 12, 2006, page 2, paragraph 1.

data stream or a direct satellite service data stream. Therefore, Applicant respectfully submits that the *prima facie* case for obviousness must fail and claim 1, as amended is patentable over Luyster and Mroczkowski, and request withdrawal of the reject and reconsideration.

Claims 10 and 22

Independent claims 10 and 22 are amended to include the limitation wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream. For the reasons present above, Applicants respectfully submits that these claims as amended are now patentable over the cited references, and request withdrawal of the rejection and reconsideration.

Claims 2-9, 11-21, and 23-24

Dependent Claims 2-9, 11-21, and 23-24 depend from allowable independent claims 1,10, and 22 and are therefore also allowable. “If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).”³

Applicant respectfully asserts that dependent Claims 2-9, 11-21, and 23-24 are allowable as well and requests reconsideration and withdrawal of the rejection.

³ See, MPEP 2143.03.

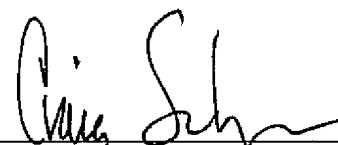
CONCLUSION

In view of the above, withdrawal of finality and reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,
Lee, Hong, Degerman, Kang & Schmadeka

Date: July 12, 2006

By: _____


Craig W. Schmoyer
Registration No. 51,007
Attorney for Applicant

Customer No. 035884